(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年4 月14 日 (14.04.2005)

PCT

(10) 国際公開番号
WO 2005/034422 A1

(51) 国際特許分類[7]: H04L 9/08, 12/14, G11B 20/10

(21) 国際出願番号: PCT/JP2004/013980

(22) 国際出願日: 2004 年9 月16 日 (16.09.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-340076 2003 年9 月30 日 (30.09.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 木谷 聡 (KITANI, Satoshi) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

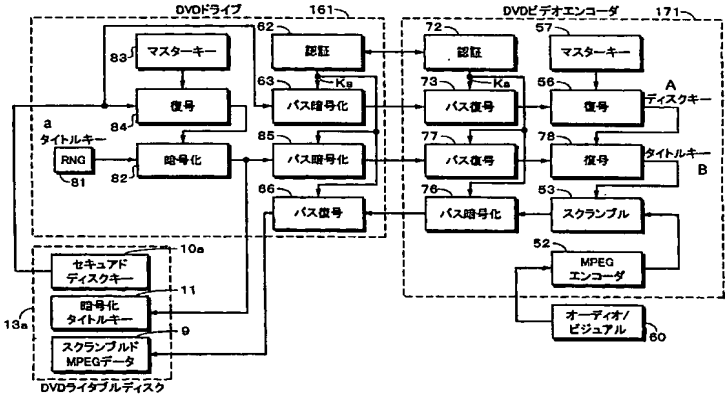
(74) 代理人: 杉浦 正知, 外(SUGIURA, Masatomo et al.); 〒1710022 東京都豊島区南池袋2丁目49番7号 池袋パークビル７階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,

[続葉有]

(54) Title: SIGNAL PROCESSING SYSTEM

(54) 発明の名称: 信号処理システム




161... DVD DRIVE
171... DVD VIDEO ENCODER
83... MASTER KEY
84... DECRYPTION
82... ENCRYPTION
a... TITLE KEY
10a... SECURED DISC KEY
11... ENCRYPTION TITLE KEY

9... SCRAMBLED MPEG DATA
13a... DVD WRITABLE DISC
62... AUTHENTICATION
63... BUS ENCRYPTION
85... BUS ENCRYPTION
66... BUS DECRYPTION
72... AUTHENTICATION
73... BUS DECRYPTION
77... BUS DECRYPTION

76... BUS ENCRYPTION
57... MASTER KEY
56... DECRYPTION
78... DECRYPTION
53... SCRAMBLE
52... MPEG ENCODER
60... AUDIO/VISUAL
A... DISC KEY
B... TITLE KEY

(57) Abstract: A writable disc (13a) where a secured disc key (10a) has been recorded in advance is used. A drive (161) includes inside itself: a random number generator (81) for generating a title key; an encrypter (82) for encrypting the generated title key with the disc key; a master key (83); and a decrypter (84) for decrypting the secured disc key with the master key. Furthermore, there are provided an authentication unit (62) for generating a session key (Ks), a bus encrypter (63) for encrypting the secured disc key with the session key (Ks), and a bus decrypter (66) for decrypting the scrambled MPEG data. Since the key for encryption is provided inside the drive, an ordinary user cannot create CSS write software as he/she desires.

(57) 要約: 予めセキュアドディスクキー１０ａが記録されているライタブルディスク１３ａが使用される。ドライブ１６１は、タイトルキーを生成する乱数発生器８１と、生成したタイトルキーをディスクキーで暗号化するエンクリプタ８２と、マスターキー８３と、セキュアドディスクキーをマスターキーで復号するデクリプタ８４とを内部に備えている。さらに、セッションキーＫｓを生成する認証部６２、セッションキーＫｓでセキュアドディスクキーを暗号化するパ

[続葉有]

WO 2005/034422 A1

SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書



スエンクリプタ６３、スクランブルドＭＰＥＧデータを復号するバスデクリプタ６６が備えられている。暗号化のための鍵がドライブ内にあるために、一般ユーザがＣＳＳ書き込みソフトウェアを勝手に作成できない。